The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
05/17/2022
05/17/2022 - UPDATED

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution.

- Safari is a graphical web browser developed by Apple.
- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- iPadOS is the successor to iOS 12 and is a mobile operating system for iPads.
- macOS Monterey is the 18th and current major release of macOS.
- macOS Big Sur is the 17th release of macOS.
- macOS Catalina is the 16th major release of macOS
- watchOS is the mobile operating system for Apple Watch and is based on the iOS operating system.
- tvOS is an operating system for fourth-generation Apple TV digital media player.
- Xcode is Apple's integrated development environment for macOS

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

May 17th – UPDATED THREAT INTELLIGENCE:
Apple is aware CVE-2022-22675 is currently being exploited in the wild.

SYSTEMS AFFECTED:

- Safari priori to 15.5
- tvOS prior to 15.5
- Xcode prior to 13.4
- macOS Catalina prior to Security Update 2022-004
- macOS Big Sur prior to 11.6.6
- macOS Monterey prior to 12.4
- iOS and iPadOS prior to 15.5
- watchOS prior to 8.6

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution in the context of the affected user. Following the MITRE ATT&CK framework, exploitation of these vulnerabilities can be classified as follows:

Tactic: *Execution* **(**TA0002**)**:

Technique: *Native API* **(**T1106**)**:

- A buffer overflow issue was addressed with improved memory handling. (CVE-2022-26741, CVE-2022-26742, CVE-2022-26749, CVE-2022-26750, CVE-2022-26752, CVE-2022-26753, CVE-2022-26754)

Technique: *Exploitation for Client Execution* **(**T1203**)**:

- An integer overflow was addressed with improved input validation. (CVE-2022-26711, CVE-2022-26775)
- An access issue was addressed with additional sandbox restrictions on third-party applications. (CVE-2022-26706)

Tactic: *Privilege Escalation* **(**TA0029**)**:

Technique: *Process Injection* **(**T1055**)**:

- A race condition was addressed with improved locking. (CVE-2022-26701)
- A race condition was addressed with improved state handling. (CVE-2022-26765)
- A memory corruption issues were addressed with improved input validation. (CVE-2018-25032, CVE-2022-26723, CVE-2022-26751, CVE-2022-26769)
- A memory corruption issues were addressed with improved memory handling. (CVE-2022-26761, CVE-2022-26762)
- A memory corruption issues were addressed with improved state management. (CVE-2022-26700, CVE-2022-26716, CVE-2022-26719, CVE-2022-26744, CVE-2022-26760, CVE-2022-26768, CVE-2022-26771, CVE-2022-26772)
- A memory corruption issues were addressed with improved validation. (CVE-2022-26714, CVE-2022-26745, CVE-2022-26764)
- A memory corruption issue was addressed with improved state management.)
- A memory initialization issue was addressed. (CVE-2022-26721, CVE-2022-26722)
- A use after free issues were addressed with improved memory management. (CVE-2022-23308, CVE-2022-26702, CVE-2022-26709, CVE-2022-26710, CVE-2022-26717, CVE-2022-26757)

Details of lower-severity vulnerabilities are as follows:

- A certificate parsing issue was addressed with improved checks. (CVE-2022-26766)
- A denial of service issue was addressed with improved input validation. (CVE-2022-0778)
- A denial of service issue was addressed with improved state handling. (CVE-2022-0530)
- A logic issue in the handling of concurrent media was addressed with improved state handling.)
- A logic issue in the handling of concurrent media was addressed with improved state handling. (CVE-2022-22677)
- A logic issues were addressed with improved state management. (CVE-2022-24765, CVE-2022-26725, CVE-2022-26731)
- A logic issue was addressed with improved validation. (CVE-2022-22665)
- An authentication issue was addressed with improved state management. (CVE-2022-26724)
- An authorization issue was addressed with improved state management. (CVE-2022-26703)
- An out-of-bounds access issue was addressed with improved bounds checking. (CVE-2022-26763)
- An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. (CVE-2022-22674)
- An out-of-bounds read issues were addressed with improved input validation. (CVE-2022-26697, CVE-2022-26718, CVE-2022-26770)
- An out-of-bounds read issue was addressed with improved bounds checking. (CVE-2022-26698)

- An out-of-bounds read was addressed with improved bounds checking. (CVE-2022-26698)
- An out-of-bounds read was addressed with improved input validation. (CVE-2022-26697)
- An out-of-bounds write issues were addressed with improved bounds checking. (CVE-2022-22675, CVE-2022-26715, CVE-2022-26720, CVE-2022-26736, CVE-2022-26737, CVE-2022-26738, CVE-2022-26739, CVE-2022-26740, CVE-2022-26743)
- An out-of-bounds write issues were addressed with improved input validation. (CVE-2022-26748, CVE-2022-26756)
- A validation issue existed in the handling of symlinks and was addressed with improved validation of symlinks. (CVE-2022-26704)
- A validation issue was addressed with improved input sanitization. (CVE-2022-22589)
- Multiple issues were addressed by updating apache to version 2.4.53. (CVE-2021-44224, CVE-2021-44790, CVE-2022-22719, CVE-2022-22720, CVE-2022-22721)
- Multiple issues were addressed by updating Vim. (CVE-2021-4136, CVE-2021-4166, CVE-2021-4173, CVE-2021-4187, CVE-2021-4192, CVE-2021-4193, CVE-2021-46059, CVE-2022-0128)
- An issue was addressed with additional permissions checks. (CVE-2022-26767)
- An issue was addressed by removing the vulnerable code. (CVE-2022-26712)
- An issue was addressed by updating to zsh version 5.8.1. (CVE-2021-45444)
- An issue was addressed with improved checks. (CVE-2015-4142)
- An issue was addressed with improved checks to prevent unauthorized actions. (CVE-2022-22663)
- An issue was addressed with improved entitlements. (CVE-2022-26727)
- An issue was addressed with improved environment sanitization. (CVE-2022-26755)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply the stable channel update provided by Apple to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Inform and educate users regarding the threats posed by hypertext links

contained in emails or attachments especially from un-trusted sources. (**M1017: User Training**)

  - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
  - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
  - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
  - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
  - o Safeguard 2.6 : Allowlist Authorized Libraries: Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
  - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048 : Application Isolation and Sandboxing**)
  - **Safeguard 4.1 : Establish and Maintain a Secure Configuration Process:** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)

- **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
- **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Apple:
https://support.apple.com/en-us/HT213253
https://support.apple.com/en-us/HT213254
https://support.apple.com/en-us/HT213255
https://support.apple.com/en-us/HT213256
https://support.apple.com/en-us/HT213257
https://support.apple.com/en-us/HT213258
https://support.apple.com/en-us/HT213260
https://support.apple.com/en-us/HT213261

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0128
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0530
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4136
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4142
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4166
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4173
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4187
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4192
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4193
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22589
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22663
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22665
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22674
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22675
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22677
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22719
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22721
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23308
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24765
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26697
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26698
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26700
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26701
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26702
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26703
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26704
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26706
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26709
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26710
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26711
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26712
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26714
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26715
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26716
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26717
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26718
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26719
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26720
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26721
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26722
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26723
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26724
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26725
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26727
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26731
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26737
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26739
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26740
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26741
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26742
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26743
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26744
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26748
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26749
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26750
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26751
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26752

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26753
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26754
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26755
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26756
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26757
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26760
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26761
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26762
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26763
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26764
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26765
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26766
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26767
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26768
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26769
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26770
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26771
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26772
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26775
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44224
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45444
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46059

May 17th – UPDATED REFERENCES:
Malwarebytes:
https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/05/update-now-apple-patches-zero-day-vulnerability-affecting-macs-apple-watch-and-apple-tv/